AMENDMENTS TO THE SPECIFICATION

I. On page 4 of the specification, please amend the paragraphs on lines 10 through 20 as follows:

The authors of Trust in Cyberspace explain the security challenge faced by today's designers of ~~application~~ applications in terms of deriving a trusted networked information system (NIS) from the integration of untrustworthy components.

A second aspect of security design problems is apparent from newspapers, periodicals and texts. Those who seek to corrupt or to interfere with the correct and reliable operation of networked information ~~system~~ systems have a structured approach to achieving their objective whereas the architects who seek to design trustworthy solutions rely largely on individualized approaches.

The effectiveness of security measures in computing solutions can be handicapped by component limitations, by ~~mis-communicatied~~ miscommunicated or misinterpreted requirements or by narrowly focused application of security technology.

II. On page 7 of the specification, please amend the paragraph on lines 3 through 9 as follows:

There have been several attempts to organize a security design process without regard to subsystems or components. These are in Sections 10.1-10.2 of ISO/IEC PDTR 15446 entitled "Information Security Techniques Guide for the Production of Protection Profiles and Security Target which is found at http://csrc.nist.gov/cc/t4/wg3/27n2449.pdf and a tool funded by the US government and made publicly available called CCTOOL which may be found at http://naip.nist.gov/tools/cctool.html. These ~~attempt~~ attempts generally fall short of the desired level of consistent security, independent of the components and subsystems.

III. On page 11 of the specification, please amend the paragraph on lines 12 through 23 as follows:

Next, at block 106, the security properties of the overall solution are determined in terms of the security subsystems identified in Fig. 3 and represented in Figs. 4-8 using the Solution Outline Activities. Then, at block 108 functional details of the security subsystems are assigned to various elements of the solution, including infrastructure, components and operations, using the SI Method Macro Design ~~Activities).~~ Activities. Following this step, at block 110 the security requirements for the solution are enumerated for each of the infrastructure, components and operations using the Common Criteria. The Common Criteria are also used at block 112 to develop assurance requirements for the solution. Finally, then, at block 114 the entire process is documented, by creating functional technology diagram(s) and documenting the requirements, rationale and guidance for component selection and systems integration and solution operation using Solution Design Activities from the SI Method as described in the SI Patent referenced above.

IV. On page 13 of the specification, please amend the paragraph on lines 2 through 16 as follows:

Fig. 3 illustrates representative components of an IT Security processes and subsystems which are described individually in detail later in connection with Fig. 4-8. These subsystems are an audit subsystem 310, an integrity subsystem 320, an access control subsystem 330, an information flow management subsystem 340 and an identity and credentials subsystem 350. The interconnection and interoperation of these systems is shown, with the effect that each of the subsystems is connected to ~~an~~ and influences the other subsystem to provide a single integrated security system of the present invention. The audit subsystem 310 is shown and described in greater detail below in connection with Fig. 4, the integrity subsystem 320 is described in greater detail in connection with Fig. 5 and the access control subsystem 330 is shown and described in detail in connection with Fig. 6 below. The information flow management system 340 is shown in detail and described in connection with Fig. 7 and the identity and credentials subsystem 350 is shown and described in connection with Fig. 8. Many elements of the various subsystems are either self-explanatory or similar from one subsystem to the next and will not be discussed in detail in connection with the various subsystems.